DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

JOHN H. HEMANN (CABN 165823)
SHIAO C. LEE (CABN 257413)
Assistant United States Attorneys

450 Golden Gate Avenue, 9th Floor
San Francisco, California 94102-3495
Telephone: (415) 436-6924
FAX: (415) 436-7234
John.hemann@usdoj.gov
Shiao.lee@usdoj.gov

NICHOLAS O. HUNTER (DCBN 1022355)
Trial Attorney, National Security Division

950 Pennsylvania Ave., NW
Washington, DC 20530
Tel: (202) 233-0986
Fax: (202) 233-2146
Nicholas.Hunter@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. UNITED MICROELECTONICS CORPORATION, INC.; FUJIAN JINHUA INTEGRATED CIRCUIT, CO., LTD.; CHEN ZHENGKUN, a.k.a. STEPHEN CHEN; HE JIANTING, a.k.a. J.T. HO; and WANG YUNGMING, a.k.a. KENNY WANG. Defendants.	CASE NO. CR 18-465 MMC UNITED STATES' REPLY IN SUPPORT OF MOTION FOR ENTRY OF PROTECTIVE ORDER

Defendants' response briefs demonstrate a lack of awareness by their counsel of the information-security threats posed by sophisticated nation-state intelligence services, particularly those of the People's Republic of China ("PRC"). But defense counsel are not alone, which is why the Director of the National Counterintelligence and Security Center recently addressed law firms to warn them that firms "both large and small are increasingly being targeted by . . . nation-state intelligence services." Hunter Decl. Ex. B at 2. Defendants' briefs also demonstrate a failure to recognize that this is not a run-of-the-mill civil intellectual property case. This is a national-security case, involving charges of economic espionage to benefit a foreign state that has aggressively sought to steal or otherwise misappropriate U.S. technology.

1. Defendants Misstate the Legal Standard Under the Economic Espionage Act

The protection of confidential information in cases brought under the Economic Espionage Act is governed by 18 U.S.C. § 1835. Using the obligatory "shall," that section mandates the entry of protections that "*may* be necessary and appropriate to preserve the confidentiality of trade secrets." 18 U.S.C. § 1835 (emphasis added). Thus, all that is required is the demonstration of a reasonable risk to trade-secret information. As demonstrated by its opening brief, the government has shown that keeping confidential information out of Hong Kong "may be necessary and appropriate to preserve" that information's confidentiality.

Jinhua incorrectly asserts (at 4) that the government must satisfy a "necessary and appropriate standard" with examples of "specific prejudice or harm" in order to impose restrictions. But the government need not establish that restrictions *are* necessary and appropriate. It only must establish that its proposed restrictions *may be* necessary and appropriate. Nor does § 1835 require a showing of "specific prejudice or harm." But even if it did, the threatened harm here is obvious: If Micron's confidential information is brought into Hong Kong, there is a substantial likelihood it will be stolen by nation-state intelligence operatives from the PRC.

Jinhua attempts to avoid the strictures of § 1835 by asserting (at 3) that, because it allegedly stole a large volume of Micron's confidential information, not all of that information can be a trade secret subject to § 1835. But Congress passed § 1835 to afford maximum protection to trade secret

information, in part by avoiding pre-trial litigation of what is and is not a trade secret. In a Manager's Report, the sponsors of the Economic Espionage Act stated: "It is important that in the early stages of a prosecution the issue whether material is a trade secret not be litigated. Rather, courts should, when entering these orders, always assume that the material at issue is in fact a trade secret." 142 Cong. Rec. 27051, 27117 (Oct. 2, 1996).

In any event, whether § 1835's mandatory and more protective provision applies or Rule 16's discretionary, good cause standard applies is of no moment. The demonstrated information-security concerns for international travel, including to Hong Kong, are good cause for limiting defendants' counsels' ability to bring confidential information there.

Jinhua relies (2-3) on *United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1998), to assert that the Court must "strike a balance" in determining defendants' access to trade secrets. *Hsu*, however, offers no support for defendants' position. The court in *Hsu* had no opportunity to address geographic restrictions, because it held that, in light of § 1835, the defendants were not entitled to the confidential information *at all*. *Id.* at 204 (trade-secrets not material to the preparation of the defense because legal impossibility is not a defense to conspiracy and attempt to steal trade secrets). Unlike in *Hsu*, the government has never sought to completely withhold trade-secret information from the defense.

2. Defendants' Attempt to Distinguish Hong Kong from the PRC Does Not Address the Information-Security Threat that Exists in Both Places

There is no dispute that it would be inappropriate for defendants' law firms to bring confidential materials into mainland China—even though both of defendants have offices there and Jinhua is located there. Despite current events, Defendants' chief argument is that Hong Kong is an entirely autonomous region that—as defendants would have it—is entirely devoid of the information-security risks that exist in mainland China. The United States government disagrees; and Micron has expressed a strong desire that the confidential information in this case not be allowed to enter that region.

As demonstrated by its initial submissions, the government does not dispute that Hong Kong and the United States have historically enjoyed friendly relations, that Hong Kong has been a more business friendly environment than mainland China, or that Hong Kong has historically enjoyed a high degree of

autonomy from mainland China. None of that is the point. The point is—as demonstrated by the recent massive protests in Hong Kong—that historical trend has begun to shift. As the State Department stated in the "[k]ey [f]indings" of its 2019 Hong Kong Policy Act Report—findings that defendants completely ignore—the Chinese mainland central government has recently begun exercising tighter control over Hong Kong, inconsistent with its international legal obligations. "The tempo of mainland central government intervention in Hong Kong affairs—and actions by the Hong Kong government consistent with mainland direction—increased, accelerating negative trends seen in previous periods." Hunter Decl., Ex. K at 2. This shift demonstrates the increased threat from PRC security and intelligence services that are active in Hong Kong. Indeed, those services are active all over the world; it is beyond any doubt that they are active in a territory of such strategic importance to the PRC government.

Despite lengthy recitations about law firms and businesses in Hong Kong and its friendly business environment, defendants offer nothing to show that PRC security and intelligence services are not active there. UMC's speculation (at 6-7) that if Hong Kong were an information-security threat, businesses there "would be forced to curtail or close their operations immediately" is pure hyperbole. Businesses would continue to do business in Hong Kong if there was a profit to be made, just as businesses from all over the world—including defendants' law firms—do business in mainland China, despite the significant counterintelligence and information-security threat posed there.

Jinhua repeatedly mischaracterizes the State Department report by asserting (at 6-7) that agents of the mainland PRC government are "not authorized to operate" in Hong Kong. But Jinhua's quotation is incomplete. The report states:

> Hong Kong maintained customs, immigration, and law enforcement authorities distinct from those of the mainland central government, whose agents were not authorized to operate in Hong Kong *except in specified instances discussed later in this report. Mainland operatives reportedly monitored some political activists, NGOs, and academics who criticized the Chinese central government's policies.*

Hunter Decl. Ex K. at 2-3 (emphasis added). Notably, the report does not state that *intelligence* or *internal security* agents are not authorized to operate in Hong Kong.

Jinhua also asserts (at 7) that it is "not aware of any incidents where [defendants' firms] physical or digital premises were broken in by Chinese intelligence agents or anyone else." But the PRC has one of the most sophisticated intelligence-gathering apparatus's in the world. In light of its ability to operate covertly, it would be shocking if defendants' firms did know about incidents of data theft by those services.

Jinhua argues (at 7) that the Office of the Director of National Intelligence's advice to leave devices at home when traveling internationally is not specific to Hong Kong. But that advice encompass all international travel, which necessarily includes travel to Hong Kong. It thus demonstrate the significant concessions the United States and Micron have already made by allowing confidential information into other countries such as Japan and Singapore. Defendants have no constitutional or statutory right to bring trade secrets that do not belong to them anywhere they want. That is especially true in a national-security case involving charges of economic espionage. Were it otherwise, hostile nation-states might actively seek economic espionage charges and attempt to use U.S. courts to illicitly gain access to secret technology owned by U.S. companies.

Jinhua also thinks it significant that Hong Kong is listed separately from mainland China with regard to Department of Commerce export-control regulations for dual-use goods. Those regulations, however, show that the Department of Commerce restricts exports to Hong Kong in nearly same manner as exports to mainland China. For example, the Department of Commerce requires a license to export to both regions goods that are controlled for national security, regional stability, and crime control. *See* 15 C.F.R. pt. 738, Supp. 1 (Commerce Country Chart).

3. Defendant's Reliance on Other Protective Orders is Unpersuasive

According to Jinhua, (10) the government's approach to high-risk countries is inconsistent because in another case the government consented to the viewing of confidential materials in Thailand. This dispute, however, is about Hong Kong, not Thailand. Just like the government's proposed protective order, the protective order in the other case did now allow the viewing of confidential information in Hong Kong.

Moreover, the protective measures required in any given case depend on a variety of factors unique to each case, including the nature of the stolen technology at issue, the desires of the victim company, and the nature of the defendant and its ties to foreign governments, to name just a few. The *Huawei* protective order that Jinhua cites (at 10)—which does not include geographic limitations—illustrates the point. Unlike this case, *Huawei* does not involve charges of economic espionage; it involves charges of conspiracy and attempt to commit theft of trade secrets under 18 U.S.C. § 1832. *See* Indictment, *United States v. Huawei Device Co.*, No. CR19-010 (W.D. Wash. Jan. 16, 2019) (D.E. 1) ("*Huawei* Indictment"). Moreover, the technology in that case involved a robot named "Tappy" that T-Mobile began developing in 2006 to test mobile phones. *See id.* ¶ 2; *see also* T-Mobile, Say Hello to T-Mobile's Tap-Happy Device Testing Robot, https://www.youtube.com/watch?v=mv69ZxKOFSw (Sept. 13, 2012). Though innovative in its own right, a robot that touches a mobile phone is not the same as the large volume of "secret-sauce" semiconductor manufacturing information stolen from Micron. And unlike this case, T-Mobile had granted Huawei access to the robot, subject to non-disclosure agreements that Huawei violated. *See Huawei* Indictment ¶¶ 11-14. Micron has never granted UMC or Jinhua such access to its trade secrets.

A far better comparison is the protective order in *United States v. You*, No. 2:19-CR-14 (E.D. Tenn.) (D.E. 29) (Hunter Decl., Ex. P). The stolen technology in that case involved secret chemical formulations for bisphenol-A free ("BPA free") food container coatings. Indictment, *United States v. You*, No. 2:19-CR-14, at ¶ 41 (E.D. Tenn. Feb. 12, 2019) (D.E. 1). The *You* protective order does not even allow defendant's counsel to possess copies of the trade-secret material in a U.S. office. Instead, viewing of trade secrets must occur on special computers maintained by the FBI. Hunter Decl., Ex. P ¶ 3. UMC and Jinhua face far less restrictions on their access to confidential information.

4. The Burden on Defendants is Minimal Compared to the Information-Security Threat Posed In Hong Kong

Defendants argue that it will be a significant burden for their non-U.S. based counsel to travel outside of Hong Kong (Jinhua Br. at 11-12). But they do not dispute that the facts of this case have no nexus to Hong Kong. And the fact that defendants' counsel have already set up "war rooms" in Hong

Kong shows that a significant amount of trial prep can still occur there without the need to transport highly technical, trade secret information there. This case will be tried in a U.S. court by U.S. defense counsel and U.S. prosecutors to vindicate the United States' national-security interests and the rights of a U.S. victim company. Defense counsels' decision to set up an overseas "war room" in the territory of the foreign state benefited by defendant's alleged economic espionage is a problem of their own making. The government has gone above and beyond by agreeing to allow the information to be brought to defense counsels' other offices in Asia.

Defendants all but admit that encryption of data brought into Hong Kong is not a sufficient protection. Instead of arguing that encryption would be secure, they argue that the government's cited public sources about breaking encryption are "generic." Defendants make no effort, however, to counter the "generic" idea that encryption is not a sufficient safeguard from a nation-state interested in breaking it, or that the PRC government is at the forefront of such efforts. And Jinhua's admission that no encryption is 100% safe is more than sufficient to establish that keeping encrypted trade secrets out of Hong Kong "may be necessary and appropriate to preserve" confidentiality. 18 U.S.C. § 1835.

5. UMC's Attempt to Portray Micron as Hypocritical is Based on Incorrect Assumptions

UMC argues that the Court should permit defense counsel to bring trade secrets to Hong Kong because—according to UMC—Micron and its law firm, Jones Day, maintain those trade secrets in China and Hong Kong, respectively. UMC's assumptions are mistaken.

First, UMC asserts (at 7) that the Court should allow defendants to review the trade secrets in Hong Kong because "Micron has a significant and established presence in Mainland China." Micron does have a presence in China. But it does not maintain the trade secrets at issue in this case in its facilities in China. Micron's counsel has confirmed that most of the trade secrets at issue in this action relate to Micron's process technology, not the DRAM design and back-end assembly that Micron performs in its Chinese facilities.

Second, UMC asserts (at 7-8) that Jones Day has offices in China and Hong Kong and "at least one of Jones Day's Hong Kong based lawyers have been involved in the Micron civil litigation against

UMC and Jinhua." That argument, however, wrongly assumes that Jones Day maintains the trade secret information at issue in this case in its Hong Kong offices. Counsel for Jones Day has confirmed that Jones Day maintains the trade secrets at issue in this case on a secure server in the United States. In addition, the Hong Kong based lawyer for Jones Day does not have access to the trade secret information on that secure server. Nor are the trade secrets at issue in this case maintained on electronic media in Jones Day's Hong Kong office.

Dated: September 27, 2019

Respectfully Submitted,

DAVID L. ANDERSON
United States Attorney

/s/ Nicholas O. Hunter
JOHN H. HEMANN
SHIAO C. LEE
Assistant United States Attorneys

NICHOLAS O. HUNTER
Trial Attorney, National Security Division